

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problems Mailbox.**

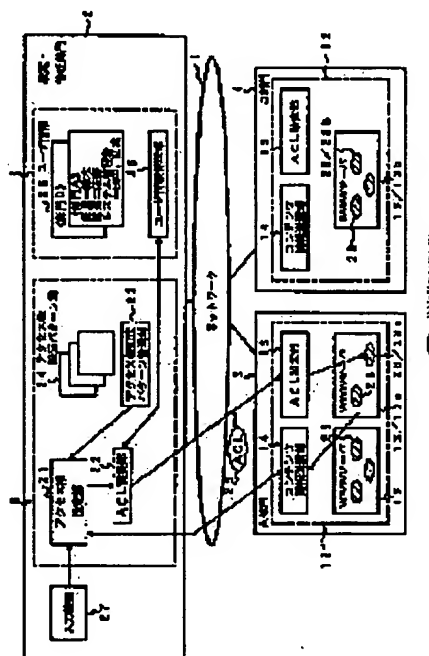
(11)Publication number : 2000-112891
(43)Date of publication of application : 21.04.2000

(51)Int.Cl.	G06F 15/00
	G06F 12/00
	G06F 13/00
	H04L 12/46
	H04L 12/28

(21)Application number : 10-288106 (71)Applicant : TOSHIBA CORP
(22)Date of filing : 09.10.1998 (72)Inventor : HASHIMOTO KEISUKE
HASEGAWA YOSHIRO

(57)Abstract:

SOLUTION: The access control setting system for setting an access right to a resource 28 in a computer 12 is provided with an access right setting pattern storing part 24 for storing one or more access right setting patterns describing persons permitted to access the resource 28 and the contents of access right and a selection means 21 for selecting one of these access right setting patterns to set the access right.



[Date of request for examination]	06.02.2001
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

Copyright (C): 1998,2000 Japan Patent Office

(11)特許出願公開番号

特開2000-112891

(P2000-112891A)

(43)公開日 平成12年4月21日(2000.4.21)

(51)Int.Cl. ¹	識別記号	F I	テーマコード [*] (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B
	5 3 7	12/00	5 3 7 A
	3 5 1	13/00	3 5 1 Z
H 0 4 L 12/46		H 0 4 L 11/00	3 1 0 C
12/28			

審査請求 未請求 請求項の数12 O.L (全 18 頁)

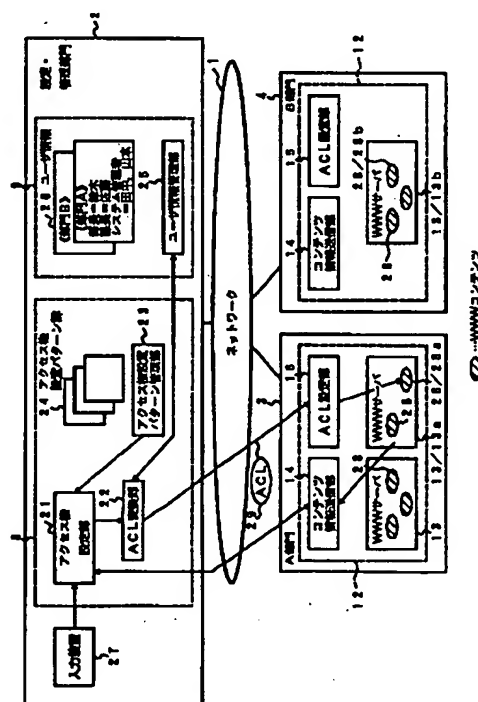
(21)出願番号	特願平10-288106	(71)出願人	000003078 株式会社東芝 神奈川県川崎市幸区堀川町72番地
(22)出願日	平成10年10月9日(1998.10.9)	(72)発明者	橋本 圭介 東京都府中市東芝町1番地 株式会社東芝 府中工場内
		(72)発明者	長谷川 義朗 東京都府中市東芝町1番地 株式会社東芝 府中工場内
		(74)代理人	100058479 弁理士 鈴江 武彦 (外6名)

(54) 【発明の名称】 アクセス制御設定システム及び記憶媒体

(57) 【要約】

【課題】 本発明は、部門やサイトに依存せず効率的にリソースへのアクセス権を設定することを可能にし、また、設定対象の計算機にその都度ログインすることなしに当該設定を可能として、ひいては設定の手間を軽減し設定ミスを防止できる。

【解決手段】 計算機 1 2 上のリソース 2 8 に対するアクセス権の設定を行うためのアクセス制御設定システムにおいて、リソースへのアクセス許諾を受ける者及びそのアクセス権内容を記述したアクセス権設定パターンを 1 以上格納するアクセス権設定パターン格納部 2 4 と、アクセス権の設定を行うために、前記アクセス権設定パターンの何れかを選択する選択手段 2 1 とを備えたアクセス制御設定システム。



【特許請求の範囲】

【請求項1】 計算機上のリソースに対するアクセス権の設定を行うためのアクセス制御設定システムにおいて、

前記リソースへのアクセス許諾を受ける者及びそのアクセス権内容を記述したアクセス権設定パターンを1以上格納するアクセス権設定パターン格納部と、

前記アクセス権の設定を行うために、前記アクセス権設定パターンの何れかを選択する選択手段とを備えたことを特徴とするアクセス制御設定システム。

【請求項2】 前記アクセス許諾を受ける者は、抽象的なユーザ名からなることを特徴とする請求項1記載のアクセス制御設定システム。

【請求項3】 前記抽象的なユーザ名に対応したグループ毎の実ユーザ名群からなるユーザ情報を、1グループ以上について格納するユーザ情報格納部と、前記選択手段にて選択されたアクセス権設定パターンに、前記ユーザ情報格納部に格納されかつアクセス権設定対象となるグループの実ユーザ名群を当てはめて、前記アクセス権の設定を行うために用いられるアクセスコントロールリストを生成するアクセスコントロールリスト生成手段を備えたことを特徴とする請求項2記載のアクセス制御設定システム。

【請求項4】 前記抽象的なユーザ名からなるアクセス権設定パターンに基づいて、前記アクセス権の設定を行うために用いられるアクセスコントロールリストを生成するアクセスコントロールリスト生成手段を備えたことを特徴とする請求項2記載のアクセス制御設定システム。

【請求項5】 前記アクセス権設定対象となるリソースを直接管理する計算機上に設けられ、かつ、前記アクセスコントロールリスト生成手段が生成したアクセスコントロールリストを当該リソースについて設定することでアクセス権設定を実行するアクセスコントロールリスト設定手段を備えたことを特徴とする請求項3又は4記載のアクセス制御設定システム。

【請求項6】 前記アクセスコントロールリストが抽象的なユーザ名からなるアクセス権設定パターンから生成されたものである場合に、前記ユーザ情報格納部に格納されかつアクセス権設定対象となるグループの実ユーザ名群に基づいて、ユーザグループ情報を作成し、当該情報を前記リソースについて設定するユーザ情報設定手段を備えたことを特徴とする請求項3乃至5記載のアクセス制御設定システム。

【請求項7】 前記アクセス権設定対象となるリソースを直接管理する計算機上に設けられ、かつ、前記アクセスコントロールリストを作成するのに用いる前記リソースの所属情報を収集するリソース情報収集手段を備え、前記選択手段は、前記リソース情報収集手段に指令して情報収集させるとともに、この情報収集対象となるリソ

ースを前記アクセス権設定対象として指定することの特徴とする請求項3乃至6のうち何れか1項記載のアクセス制御設定システム。

【請求項8】 前記選択手段は、前記リソースを直接管理する計算機とは異なる計算機上に設けられ、両計算機間の情報の授受はネットワークを介して行うことを特徴とする請求項1乃至7のうち何れか1項記載のアクセス制御設定システム。

【請求項9】 計算機上のリソースに対するアクセス権を設定させるためのアクセス制御設定システムを制御するプログラムであって、

前記リソースへのアクセス許諾を受ける者及びそのアクセス権内容を記述したアクセス権設定パターンを1以上記憶させた記憶手段から当該パターンを読み出させるアクセス権設定パターン管理手段と、

前記アクセス権を設定させるために、前記アクセス権設定パターンの何れかを選択させる選択手段とを有するプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項10】 前記アクセス許諾を受ける者は、抽象的なユーザ名からなることを特徴とする請求項9記載の記憶媒体。

【請求項11】 前記抽象的なユーザ名に対応したグループ毎の実ユーザ名群からなるユーザ情報を、1グループ以上について記憶させた記憶手段からユーザ情報を読み出させるユーザ情報管理手段と、

前記選択手段にて選択されたアクセス権設定パターンに、前記ユーザ情報格納部に格納されかつアクセス権設定対象となるグループの実ユーザ名群を当てはめさせて、前記アクセス権の設定を行うために用いられるアクセスコントロールリストを生成させるアクセスコントロールリスト生成手段を備えたことを特徴とする請求項10記載のアクセス制御設定システム。

【請求項12】 前記抽象的なユーザ名からなるアクセス権設定パターンに基づいて、前記アクセス権の設定を行うために用いられるアクセスコントロールリストを生成させるアクセスコントロールリスト生成手段を有するプログラムを記憶したコンピュータ読み取り可能な請求項10記載の記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明はアクセス制御設定システム及び記憶媒体、特に複数の部門あるいはサイトに分散した計算機上のリソースに対するアクセス権の設定を行うのに適したアクセス制御設定システム及び記憶媒体に関するものである。

【0002】

【従来の技術】 近年は計算機同士が接続されてネットワークが形成され、ある計算機から他の計算機にアクセスすることが容易となり、また、単一の計算機を複数人が

使用することもある。したがって、計算機上のリソース（ファイルシステム上のファイル、WWWサーバ上のWWWコンテンツ、各種デバイス等）に対するアクセスを管理することが重要になってきている。

【0003】このような計算機上のリソースに対するアクセス権を設定する場合には、そのリソースを管理するサーバあるいはOS（オペレーティングシステム）等に対して、それぞれ個別にその権限を設定する必要がある。この設定を行うには、設定対象の計算機にログインして設定作業を行うのが一般的である。

【0004】具体的には、各サーバ等に対し、「ユーザ1に対しては読み出しと書き込みを許可し、ユーザ2、ユーザ3、ユーザ4に対しては読み出しのみを許可する」というような形式でアクセス権情報（以下、ACL（アクセスコントロールリスト）ともいう）が個別に設定される。

【0005】

【発明が解決しようとする課題】設定されるアクセス権情報は「システム管理者には読み出しと書き込みを許可するが、一般ユーザには読み出しのみ許可する」等のような一定のパターンに当てはまる場合が多い。

【0006】しかし、「システム管理者」や「一般ユーザ」に対応する実際のユーザは、部門あるいはサイトごとに異なっている。例えば、部門Aでは「システム管理者＝ユーザa、一般ユーザ＝ユーザb、ユーザc、ユーザd」であり、部門Bでは「システム管理者＝ユーザα、一般ユーザ＝ユーザβ、ユーザγ」であるかのごとくである。

【0007】従来のアクセス権設定方法では、各部門等でその構成メンバが異なることからして当然に、アクセス権設定対象のリソース毎にそれぞれ個別のアクセス権を設定する必要がある。

【0008】上記例に当てはめれば、部門Aが保有する計算機上のリソースに対しては、「ユーザaに対しては読み出しと書き込みを許可し、ユーザb、ユーザc、ユーザdに対しては読み出しのみを許可する」というアクセス権を設定する。また、部門Bが保有する計算機上のリソースに対しては、「ユーザαに対しては読み出しと書き込みを許可し、ユーザβ、ユーザγに対しては読み出しのみを許可する」というアクセス権を設定する。

【0009】このように、設定されるべきアクセス権情報のパターンが同一であっても、実際にはそれぞれ異なるアクセス権情報に対応した権限設定を行う必要があるため、アクセス権設定者の負担を軽減するのが困難である。

【0010】また、複数の部門あるいはサイトに分散した計算機が連携して処理を行うような分散処理システムにおいては、各計算機上のリソースに対してアクセス権を設定してアクセス制御を行い得るようにするために、アクセス権設定者の負担は過大なものとなる。アクセス

権設定者は、この設定のために各計算機に一々ログインする等し、ログインした計算機上で個別のアクセス権設定処理を行う必要があるからである。

【0011】本発明は、このような実情を考慮してなされたもので、部門やサイトに依存せず効率的にリソースへのアクセス権を設定することを可能にし、また、設定対象の計算機にその都度ログインすることなしに当該設定を可能として、ひいては設定の手間を軽減し設定ミスを防止できるアクセス制御設定システム及び記憶媒体を提供することを目的とする。

【0012】

【課題を解決するための手段】上記課題を解決するために、請求項1に対応する発明は、計算機上のリソースに対するアクセス権の設定を行うためのアクセス制御設定システムについてなされたものである。

【0013】このシステムには、アクセス権設定パターン格納部が設けられ、同格納部にリソースへのアクセス許諾を受ける者及びそのアクセス権内容を記述したアクセス権設定パターンが1以上格納されている。

【0014】そして、アクセス権の設定を行うために、選択手段によって、アクセス権設定パターンの何れかが選択される。このように、このアクセス権設定パターンを用いることで、部門やサイトに依存せず効率的にリソースへのアクセス権を設定することができる。

【0015】次に、請求項2に対応する発明は、請求項1に対応する発明において、アクセス許諾を受ける者は、抽象的なユーザ名からなっている。したがって、部門等における役職名等を抽象的なユーザ名に対応させることで、より一層、部門やサイトに依存しないアクセス権設定が容易なものとなる。

【0016】次に、請求項3に対応する発明は、請求項2に対応する発明において、ユーザ情報格納部が設けられ、同格納部に抽象的なユーザ名に対応したグループ毎の実ユーザ名群からなるユーザ情報が1グループ以上について格納されている。

【0017】また、アクセスコントロールリスト生成手段が設けられ、上記選択手段にて選択されたアクセス権設定パターンに、ユーザ情報格納部に格納されかつアクセス権設定対象となるグループの実ユーザ名群が当てはめられ、アクセス権の設定を行うために用いられるアクセスコントロールリストが生成される。

【0018】したがって、設定者は一々アクセスコントロールリストを記述する必要がなく、アクセス権設定が一層容易なものとなり設定者の負荷が低減される。特に、アクセス権設定対象となるリソースが多数の場合、設定者の負荷低減効果大きい。

【0019】次に、請求項4に対応する発明は、請求項1～3に対応する発明において、アクセスコントロールリスト生成手段が設けられ、抽象的なユーザ名からなるアクセス権設定パターンに基づいて、アクセス権の設定

を行うために用いられるアクセスコントロールリストが生成される。

【0020】したがって、設定者は一々アクセスコントロールリストを記述する必要がなく、アクセス権設定が一層容易なものとなり設定者の負荷が低減される。次に、請求項5に対応する発明は、請求項4に対応する発明において、アクセス権設定対象となるリソースを直接管理する計算機上にアクセスコントロールリスト設定手段が設けられる。

【0021】このアクセスコントロールリスト設定手段により、アクセスコントロールリスト生成手段が生成したアクセスコントロールリストが当該リソースについて設定されアクセス権設定が実行される。

【0022】したがって、リソース管理計算機上にて自動的にアクセスコントロールリストを設定させることができる。これにより、アクセス権設定のために当該計算機に一々ログインする必要をなくすことができ、ひいてはアクセス権設定者の労力を低減させることができる。

【0023】次に、請求項6に対応する発明は、請求項4又は5に対応する発明において、アクセスコントロールリストが抽象的なユーザ名からなるアクセス権設定パターンから生成されたものである場合に、ユーザ情報設定手段によって、ユーザ情報格納部に格納されかつアクセス権設定対象となるグループの実ユーザ名群に基づいて、ユーザグループ情報が作成され、当該情報がリソースについて設定される。

【0024】したがって、人事異動等でグループ内のメンバーが変更された場合でも、アクセス権設定の実質内容を容易に対応させることができる。次に、請求項7に対応する発明は、請求項4～6に対応する発明において、アクセス権設定対象となるリソースを直接管理する計算機上にリソース情報収集手段が設けられている。

【0025】このリソース情報収集手段によって、アクセスコントロールリストを作成するのに用いる前記リソースの所属情報が収集される。さらに、選択手段からは、リソース情報収集手段に対して情報収集させる旨が指令され、この情報収集対象となるリソースがアクセス権設定対象として指定される。

【0026】したがって、アクセス権設定について選択手段からの集中管理を行うことができる。次に、請求項8に対応する発明は、請求項1～7に対応する発明において、選択手段は、リソースを直接管理する計算機とは異なる計算機上に設けられ、両計算機間の情報の授受はネットワークを介して行われる。

【0027】したがって、アクセス権設定者は選択手段が設けられた計算機から、全てのリソースに対するアクセス権設定をリソース管理計算機にログインすることなく容易に行うことができる。これにより、設定者の負担は低減される。

【0028】次に、請求項9に対応する発明は、請求項

1に対応する発明を1乃至複数のコンピュータに実現させるプログラムを記憶した記憶媒体である。この記憶媒体から読み出されたプログラムにより制御されるコンピュータは、請求項1のアクセス制御設定システムとして機能する。

【0029】次に、請求項10に対応する発明は、請求項2に対応する発明を1乃至複数のコンピュータに実現させるプログラムを記憶した記憶媒体である。この記憶媒体から読み出されたプログラムにより制御されるコンピュータは、請求項2のアクセス制御設定システムとして機能する。

【0030】次に、請求項11に対応する発明は、請求項3に対応する発明を1乃至複数のコンピュータに実現させるプログラムを記憶した記憶媒体である。この記憶媒体から読み出されたプログラムにより制御されるコンピュータは、請求項3のアクセス制御設定システムとして機能する。

【0031】次に、請求項12に対応する発明は、請求項4に対応する発明を1乃至複数のコンピュータに実現させるプログラムを記憶した記憶媒体である。この記憶媒体から読み出されたプログラムにより制御されるコンピュータは、請求項4のアクセス制御設定システムとして機能する。

【0032】

【発明の実施の形態】以下、本発明の実施の形態について説明する。

（発明の第1の実施の形態）図1は本発明の第1の実施の形態に係るアクセス制御設定システムを適用する計算機システムの構成例を示すブロック図である。

【0033】この計算機システムは、ネットワーク1を介して設定・管理部門2、A部門3、B部門4、C部門5、...の各部門のLANが接続されて構成されている。設定・管理部門2のLANは、ルータ6を介してネットワーク1に接続されるとともに、そのデータ伝送路7に設定管理サーバ8とディレクトリサーバ9とが接続されて構成されている。この設定・管理部門2は、アクセス権の設定や管理を行う部門である。

【0034】各部門3、4、5、...例えばA部門3のLANは、ルータ10を介してネットワーク1に接続されるとともに、そのデータ伝送路11に複数の計算機12が接続されて構成されている。LANに接続された各計算機12には、WWWサーバ13、コンテンツ情報送信部14及びACL設定部15が設けられている。本実施形態では、各部門3、4、5、...の各計算機12におけるリソースがアクセス権設定される対象となる。

【0035】図2は本実施形態におけるアクセス制御設定システムの機能構成を示すブロック図である。このアクセス制御設定システムは、設定・管理部門2に設けられたアクセス権設定部21、ACL変換部22、アクセス権設定パターン管理部23、記憶装置（図示せず）に

格納されたアクセス権設定パターン群24、ユーザ情報管理部25及び記憶装置(図示せず)に格納されたユーザ情報26と、各部門の計算機12に設けられたコンテンツ情報送信部14及びACL設定部15をその主要構成としている。

【0036】設定・管理部門2における上記構成のうち、本実施形態では、設定管理サーバ8に、アクセス権設定部21、ACL変換部22、アクセス権設定パターン管理部23及びアクセス権設定パターン群24が設けられている。また、ディレクトリサーバ9には、ユーザ情報管理部25及びユーザ情報26が設けられている。なお、これらの各構成は、設定・管理部門2に配置されるのであれば、同一の計算機上に設けても構わないし、さらに多数の計算機上に分散して設けてもよい。

【0037】アクセス権設定部21は、入力装置27を介してアクセス権設定者の入力を受け付け、各部門3等における計算機12上のWWWサーバ13に対し、設定・管理部門2からのアクセス権設定処理を可能とする。

【0038】このためにアクセス権設定部21は、計算機12上のコンテンツ情報送信部14からコンテンツ情報を受信すると共に、アクセス権設定パターン管理部23を介してアクセス権設定パターン群24からアクセス権設定パターンを取得する。さらに取得した設定パターン及び権限設定対象情報をACL変換部22に与えて、同変換部22にACL作成を依頼する。

【0039】アクセス権設定パターン管理部23は、アクセス権設定パターン群24を管理し、アクセス権設定部21の要求に応じてアクセス権設定パターンを登録、検索、削除等する。

【0040】アクセス権設定パターン群24は、図3に示すようなアクセス権の設定パターンの集合である。図3はアクセス権設定パターン群の一例を示す図である。

【0041】同図には二つの設定パターンが例示されている。パターン#1は、「部長と課長に読み出し権限を与え、システム管理者には読み出し権限と実行権限を与える。」というパターンである。また、パターン#2は、「部長と課長に読み出し権限と実行権限を与え、一般部員には読み出し権限のみを与える。」というパターンである。

【0042】ここで、図3における「部長」「課長」「システム管理者」及び「一般部員」は、抽象的なユーザ名であり実際にアクセス権を設定する対象となるユーザではない。この抽象的なユーザ名から実際のユーザ名への変換は、ユーザ情報26に基づいて行われるようになっていく。

【0043】ユーザ情報管理部25は、ユーザ情報26を管理し、同情報を登録、検索又は削除等する。本実施形態では同管理部25の機能は、LDAP(Light weight Directory Access Protocol)に準拠したディレクトリサーバ機能で

実現される。なお、同様な機能であれば他の方法で実現してもよい。また、ディレクトリサーバとは、LDAP等により会社や研究機関等における人員の情報を集中的に管理するための計算機であり、特に図示しない他の入出力手段により、常時最新の部門情報や個人情報登録更新されている。

【0044】ユーザ情報26は、図4に示すようなユーザ名(ユーザID)と抽象的なユーザ名(役職など)の対応表に相当する情報がディレクトリサーバに管理されたものである。

【0045】図4はある部門(A部門)のユーザ情報の例を示す図である。図5は他の部門(B部門)のユーザ情報の例を示す図である。次に、ACL変換部22は、アクセス権設定部21からのACL作成指令を受けると、アクセス権設定部21から取得した部門名により、ユーザ情報管理部25に依頼して対応するユーザ情報を取り出す。さらに、当該ユーザ情報をアクセス権設定部21より取得した設定パターンに当てはめ、WWWコンテンツ28に実際に設定するアクセス権情報(アクセスコントロールリスト:ACL)を生成する。

【0046】図6はACL変換部により生成されるACLの例を示す図である。同図(a)は、ACLファイルの具体的な内容例を示している。ここで"path"は、アクセス権設定対象となる計算機上のパス情報を示し、"allow"は読出や書込、実行等の許可の内容を示す。さらに"user"は、ある"allow"の対象となる具体的なユーザ名を示している。

【0047】図6(b)及び図6(c)には、図3に示すアクセス権設定パターン群24のパターン#1に対し、ACL変換部22によりそれぞれ図4及び図5のユーザ情報が当てはめられた例が示されている。なお、同図(b)、(c)に示す内容が同図(a)のような情報に変換されてACLファイルとなる。

【0048】例えば図6(b)の場合では、設定パターン#1がA部門3が保有するWWWサーバ13a上のWWWコンテンツ28aに設定する場合が想定されている。すなわちアクセス権

部長=読み出し権限

課長=読み出し権限

システム管理者=読み出し権限、実行権限

に対して、「部長→鈴木」「課長→佐藤」「システム管理者→高橋、田中」という変換がACL変換部22にて施され、図6(b)に示す内容のACLファイルが作成されて、A部門に送信される。このACLは後述するように計算機12上のACL設定部15によって、WWWコンテンツ28aに設定される。

【0049】同様に、設定パターン#1を、B部門4が保有するWWWサーバ13b上のWWWコンテンツ28bに設定した場合には、図6(c)に示す内容のACLファイルが作成されて、B部門4に送信される。

【0050】このACLファイルが送信される各計算機12に設けられた構成要素について説明する。WWWサーバ13(13a、13bを含む)は、各計算機12に設けられ、動作するワールドワイドウェブ用のサーバソフトウェアである。WWWサーバ13は、一つの計算機12上に一つに限らず複数設けられてもよい。また、各WWWサーバ13は、リソースとしてのWWWコンテンツ28(28a、28bを含む)を1以上保持している。なお、本実施形態ではアクセス権の設定対象をWWWサーバ上のWWWコンテンツの場合で説明しているが、アクセス権の設定手段を持つリソース(例えばあるOS上のコンテンツ)であれば、対象は特に限定しない。

【0051】コンテンツ情報送信部14は、アクセス権設定部21から指定されたWWWサーバ13上のコンテンツ28のコンテンツ情報として、ファイル名や現在設定されているアクセス権等を送信する。

【0052】ACL設定部15は、ACL変換部22より受け取ったアクセス権情報(ACL29)を設定対象のWWWコンテンツに設定する。なお、請求項における選択手段には、例えばアクセス権設定部21が対応する。また、アクセス権設定パターン格納部には、例えばアクセス権設定パターン群24を格納するサーバ8上の記憶手段が対応する。さらに、ユーザ情報格納部には、例えばユーザ情報26を格納するサーバ9上の記憶手段が対応する。

【0053】また、請求項におけるリソース情報収集手段には、例えばコンテンツ情報送信部14が対応する。次に、以上のように構成された本実施形態におけるアクセス制御設定システムの動作について図2及び図7を用いて説明する。

【0054】図7は本実施形態のアクセス制御設定システムの動作を示す流れ図である。同図に示すように、まず、設定・管理部門2において、設定者からのアクセス権設定部21に対する入力により、どのWWWサーバ13のアクセス権を設定するかが選択される(s1)。ここでは、A部門3が保有するWWWサーバ13aが選択されたと仮定する。

【0055】次に、A部門3のコンテンツ情報送信部14に対し、選択されたWWWサーバ13aのコンテンツ情報を送信するように、アクセス権設定部21により司令される(s2)。

【0056】この指令を受けたコンテンツ情報送信部14によって、WWWサーバ13a上のコンテンツ情報が取得され、アクセス権設定部21に対して同情報が送信される(s3)。

【0057】コンテンツ情報を受け取ったアクセス権設定部106からアクセス権設定パターン管理部23に対し、アクセス権設定パターン一覧を送信するよう司令される(s4)。

【0058】アクセス権設定パターン管理部23によりアクセス権設定パターン群24が読み込まれ、アクセス権設定部21に送信される(s5)。このアクセス権設定パターン一覧は表示装置(図示せず)上に表示される。設定者は、この表示を確認しながらアクセス権設定の対象となるコンテンツ28aと、同コンテンツに設定されるべきアクセス権設定パターンとをアクセス権設定部21に選択入力する(s6)。

【0059】ステップs6で選択された各情報は、当該入力がなされたアクセス権設定部21からACL変換部22へ送信される(s7)。なお、どの部門であるかという情報は選択コンテンツの情報に含まれている。

【0060】設定対象となるWWWサーバ13aはA部門3に含まれているため、ACL変換部22からユーザ情報管理部25に対し、A部門3のユーザ情報を送信する旨の司令がなされる(s8)。

【0061】この指令を受けたユーザ情報管理部25によって、ユーザ情報26からA部門3のユーザ情報が検索され、検索情報がACL変換部22へ送信される(s9)。

【0062】次に、ACL変換部22によりアクセス権設定パターンの抽象ユーザ名に受信したユーザ情報が適用され、WWWコンテンツ13aに設定する実際のACL(図6(a)参照)に変換される(s10)。ACLへの変換は、上記のようにアクセス権設定パターンにユーザ情報を代入することによって実行される。なお、作成されるACLには、どのアクセス権設定パターンを選択したかを特定できる情報(パターン番号等)がACLのコメント等の形で含まれるようになっている。

【0063】さらに、ステップs10で生成されたACLは、設定対象のWWWサーバ13aで使用できるフォーマットに従っている。ACLのフォーマットはWWWサーバ製品によって異なるが、各フォーマット情報は、ACL変換部22が保持しており、各WWWサーバ13にそれぞれ対応してACLが生成される。

【0064】次に、生成されたACL29はネットワーク1を介してACL変換部22からA部門3における計算機12のACL設定部15に送信される(s11)。計算機12に送信されたACL29は、ACL設定部15によって、対象となるWWWサーバ13aのコンテンツ28aに対して設定されることとなる(s12)。

【0065】以上のようにしてコンテンツ28に対してACLが設定されるが、当該ACL設定後、そのコンテンツ28(例えばコンテンツ28a)に対するアクセス制御は具体的には以下のようにして行われる。ここで、各ユーザの属性情報(ユーザ名やパスワードの情報など)がディレクトリサーバ9に登録されているものとする。

【0066】あるユーザがWWWサーバ13aのコンテンツ28aへアクセスしようすると、WWWサーバ1

3aがユーザに対してユーザ名とパスワードの入力を要求する。ユーザ名とパスワードをWWWサーバ13aが受け取ると、WWWサーバ13aがディレクトリサーバ9に当該ユーザのユーザ情報を問い合わせ、ユーザが入力したユーザ名とパスワードの組が正しく登録されているものであるかどうかを調べる（この処理を一般に「ユーザ認証」と言う）。正しく登録されていることが確認された場合、次に、WWWサーバ13aが、ここで得たユーザ名とACLで設定されている権限者名を比較し、一致する名前があればACLに設定されている権限に応じてコンテンツ28aへのアクセスを許可する。

【0067】 上述した本発明の実施の形態に係るアクセス制御設定システムによれば、以下の効果が奏される。まず、アクセス権設定部21からの情報に基づき、ACL変換部22によりACLを自動生成するようにしたので、アクセス権設定パターンを選択するだけでACLの設定を行うことができ、ACLを設定するための手間が軽減される。特に、アクセス権の内容を設定のたびに設定者が一々ACLを記述する必要がないので、記述ミスによる設定不備も防止できる。

【0068】 また、アクセス権設定パターン群24における各パターンは抽象的なユーザ名を用いて記述されているので、所属するユーザが異なっている複数の部門あるいはサイトに対しても、同一のアクセス権設定パターンを利用することができる。したがって、システム全体で必要とするアクセス権のパターン数が大幅に減少し、管理コストが軽減され、これによりアクセス権設定コストの軽減も図れる。

【0069】 さらに、本実施形態における各処理は、アクセス権の設定時のみで完結している。したがって、WWWサーバ上のコンテンツへのアクセス時に追加的な処理が発生することはなく、実行時（運用時：リソースにアクセスするとき）の性能劣化は起こらない。

【0070】 また、ACL変換部22から各部門の計算機12へACLを配送する機構を備えているので、ネットワーク1上に分散配置されたWWWサーバ13上のコンテンツに対するアクセス権の設定を、一個所（設定・管理部門2）で集中的に行うことができる。これにより、アクセス権設定者が設定対象の計算機12にその都度ログインする等の手間が軽減される。なお、この処理を実現するのに、実行時（コンテンツへのアクセス時）におけるWWWサーバのアクセス権確認機構などは、従来のまま変更や追加を行う必要はない。

【0071】 また、ディレクトリサーバ9にてユーザ情報を一括管理しているので、人事異動等によりユーザ情報に変更があった場合でも、ACLに付加されたアクセス権設定パターンに関する情報（パターン番号等）を利用してACLの再変換を行うのみで、ユーザ情報の変更を容易に反映させることができる。なお、アクセス権設定部21は、再変換時の選択が可能のように構成され、

同選択がなされた場合には、コンテンツ情報に上記パターンに関する情報を含めるようにコンテンツ情報送信部14に指令する。さらに、このパターンに関する情報を用いて自動的にACL変換部22への付与情報が取得され、ACL生成指令がなされる。

（発明の第2の実施の形態） 第1の実施形態ではACLパターンを設定・管理部門側でACLに変換してからWWWサーバに配布していたが、本実施形態はACLパターンからの変換をWWWサーバ側で行うものである。

【0072】 図8は本発明の第2の実施の形態に係るアクセス制御設定システムの機能構成を示すブロック図であり、図2と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【0073】 このアクセス制御設定システムにおいては、ユーザ情報管理部25及びユーザ情報26a、26b、...と、ACL変換部22とが各部門3、4、...に設けられる他、第1の実施形態と同様に構成されている。

【0074】 各ユーザ情報26a、26b、...は、それぞれの部門3、4、...についての情報である。ユーザ情報及びユーザ情報管理部25は、部門LANにおける各計算機12、あるいはその部門に関する情報管理や各種処理を行うサーバ計算機（部門管理計算機31）に設けられている。何れの場合でもACL変換部22は、ユーザ情報管理部25に依頼してユーザ情報を取得できるように構成される。

【0075】 次に、以上のように構成された本実施形態におけるアクセス制御設定システムの動作について図8及び図9を用いて説明する。図9は本実施形態のアクセス制御設定システムの動作を示す流れ図である。

【0076】 同図に示す処理のうち、ステップt1からステップt6間での処理は、第1の実施形態の図7におけるステップs1からステップs6と同様であるので説明を省略する。なお、本実施形態においても、A部門3におけるWWWサーバ13aのコンテンツ28aについてアクセス権を設定する場合について説明する。

【0077】 設定者によるアクセス権設定部21に対する選択入力終了すると（t6）、アクセス権設定の対象となるコンテンツ28aの指定情報と、同コンテンツについて設定されるべきアクセス権設定パターンの情報と（ACLパターン32）が、設定管理サーバ8のアクセス権設定部21からネットワーク1を介してA部門3における計算機12上のACL変換部15へ送信される（t7）。

【0078】 このACLパターン32を受け取ったACL変換部22からA部門3のユーザ情報管理部25に対し、A部門3のユーザ情報を送信する旨の司令がなされる（t8）。

【0079】 この指令を受けたユーザ情報管理部25によるユーザ情報の取得、さらにはユーザ情報及び設定パ

ターンに基づくACL 29の生成が、第1の実施形態における図7のステップs 8, s 9, s 10と同様にして行われる(図9: t 8, t 9, t 10)。

【0080】A部門のACL変換部22にて生成されたACL 29は、A部門3内においてACL設定部15に送信される(t 11)。このACL 29を受信したACL設定部15により、第1の実施形態と同様にして、当該ACL 29はWWWサーバ13a上のコンテンツ28aに設定される(t 12)。

【0081】以上のようにしてACL設定されたコンテンツ28に対し、実際のシステム運用時にいかにしてアクセス制御されるかは第1の実施形態の場合と同様であり、その具体的な説明はここでは省略する。

【0082】上述した本発明の実施の形態に係るアクセス制御設定システムによれば、第1の実施形態と同様な効果が得られる他、更に以下の効果が奏される。まず、ネットワーク1を介して送信されるデータがACLパターン32のみ(設定パターン情報及びコンテンツ指定情報)となるため、第1の実施形態の場合に比べ、送信データ量の軽減を図ることができる。

【0083】また、ACL 29への変換処理を各WWWサーバ13側で行うことにより、第1の実施形態の場合に比べ、ACL変換作業の負荷分散を図ることができる。

(発明の第3の実施の形態) 第2の実施形態では、ユーザ情報管理部及びユーザ情報を各部門に設置するようにしたが、本実施形態では、ACL変換部は各部門に設置しユーザ情報管理部及びユーザ情報は、設定・管理部門2に一括して設置するものである。

【0084】図10は本発明の第3の実施の形態に係るアクセス制御設定システムの機能構成を示すブロック図であり、図2又は図8と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【0085】このアクセス制御設定システムは、ユーザ情報管理部25及びユーザ情報26が第1の実施形態と同様に設定・管理部門2のディレクトリサーバ9に設けられる他、第2の実施形態と同様に構成されている。

【0086】このように構成された本実施形態のアクセス制御設定システムにおいては、ACL変換部22による対象部門のユーザ情報の問合せがネットワーク1を介して設定・管理部門2のユーザ情報管理部25に対して行われる点を除けば、第2の実施形態と同様に動作する。

【0087】以上のようにしてACL設定されたコンテンツ28に対し、実際のシステム運用時にいかにしてアクセス制御されるかは第1の実施形態の場合と同様であり、その具体的な説明はここでは省略する。

【0088】上述した本発明の実施の形態に係るアクセス制御設定システムによれば、第2の実施形態と同様な

効果が得られる他、ユーザ情報26の管理を設定・管理部門2にて集中的に行われるため、第1の実施形態と同様に、各部門3, 4, ... におけるユーザ情報管理資源の設置コストやユーザ情報管理コスト自体を削減することができる。

【0089】なお、本実施形態では、ACLを生成するたびに設定・管理部門へユーザ情報の問い合わせを行うオーバーヘッドが生じトラフィックが増えることになるが、第1及び第2の実施形態では、このようなトラフィック増加を防止することができる。

(発明の第4の実施の形態) 上記各実施形態では、生成されるアクセス権として、個々のユーザに対するアクセス権の形で表現する場合を説明したが、本実施形態は、単数または複数のユーザから構成されるユーザグループ単位でアクセス権を設定するものである。

【0090】図11は本発明の第4の実施の形態に係るアクセス制御設定システムの機能構成を示すブロック図であり、図2と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【0091】このアクセス制御設定システムは、ACL変換部22'の機能が修正される他、第1の実施形態と同様に構成されている。ACL変換部22'は、設定する権限者としてユーザ名を使用する代わりに、単数または複数のユーザから構成されるユーザグループを使用するようなACLを生成する点が、第1の実施形態と異なっている。また、第1～第3の実施形態では特に説明しなかったが、ユーザ情報管理部25は、ユーザグループ名と、そのユーザグループにどのユーザが所属しているかの情報も合わせて管理している。

【0092】図12は本実施形態のACL変換部により生成されるACLファイルの例を示す図である。同図に示すように、図6(a)ではユーザ名が入る部分にユーザグループ名52が記述されている。

【0093】なお、本実施形態におけるWWWサーバ13は、ユーザグループ単位でのACLの設定機能やユーザグループの管理機能を提供するものである。次に、以上のように構成された本実施形態におけるアクセス制御設定システムの動作について説明する。

【0094】ユーザグループ名によるACL設定がなされる部分を除けば、本実施形態の動作は第1の実施形態と同様であるので、その点は説明を省略する。例えばA部門3のユーザ情報が図4のとおりであり、A部門3のWWWサーバ13a上のコンテンツ28aに対して図3のアクセスパターン#1を設定する場合を考える。

【0095】まず、ユーザ情報管理部25が、図4に示す情報に対応して、以下のようなユーザグループの定義を管理しているものとする。

- ・「部門Aの部長」グループ=鈴木が所属
- ・「部門Aの課長」グループ=佐藤が所属
- ・「部門Aのシステム管理者」グループ=高橋、田中が

所属

ここでは、ユーザグループ名の命名規則として、「抽象ユーザ名の前に対象部門名を付加する」という規則を採用している。命名規則は別の規則を採用しても問題ないが、どのような命名規則を採用するかは、ACL変換部22'とユーザ情報管理部25で共有されている必要がある。

【0096】第1の実施形態ではACL変換部22にてアクセス権設定パターンの抽象ユーザ名が実ユーザ名に展開されるが、本実施形態のACL変換部22'では、上記命名規則に従ってユーザグループ名に展開される。すなわち、

部長＝読み出し権限

課長＝読み出し権限

システム管理者＝読み出し権限、実行権限
というアクセス権設定パターンが、

A部門の部長＝読み出し権限

A部門の課長＝読み出し権限

A部門のシステム管理者＝読み出し権限、実行権限
というACLに変換される。

【0097】同様に、同じアクセス権設定パターン#1をB部門のWWWサーバ13に設定する場合は、

B部門の部長＝読み出し権限

B部門の課長＝読み出し権限

B部門のシステム管理者＝読み出し権限、実行権限
というACLに変換される。

【0098】この変換されたACLは計算機12のACL設定部15によってWWWサーバ13aのコンテンツ28aに設定される。以上のようにしてACL設定されたコンテンツ28に対し、実際のシステム運用時にいかにしてアクセス制御されるかは、基本的には第1の実施形態の場合と同様であるが、相違する部分もあるのでその点について説明する。

【0099】すなわち、WWWサーバ13がユーザ認証を完了した後、ACLに設定されている権限者を確認する場合、ACLにはユーザグループ名が記載されているため、このユーザグループにどのユーザが所属しているかを、ディレクトリサーバ9に問い合わせることにより確認する。例えば、「部門Aのシステム管理者」というユーザグループに対しては、「高橋、田中」というユーザ名のリストが得られる。ユーザ認証の結果確認されたユーザ名（コンテンツにアクセスしようとしているユーザ）が、ここで得られたユーザ名のリストに含まれているかを確認し、含まれていれば権限者であると認定し、ACLに設定されている権限に応じてコンテンツ28に対するアクセスを許可する。

【0100】上述した本発明の実施の形態に係るアクセス制御設定システムによれば、第1の実施形態と同様な効果が得られる他、アクセス権設定パターンを実ユーザではなくユーザグループに展開するようにしたので、人

事異動などによりユーザ情報が変更になった場合でも、ユーザグループの定義を変更するだけでACLの再生成などの作業は不要とすることができる。

【0101】なお、本実施形態は、第1の実施形態に対応させる場合を説明したが、本実施形態におけるユーザグループ単位でACLを設定する方法は、他の第2、第3実施形態に対しても同様に適用することができる。

（発明の第5の実施の形態）上記各実施形態では、実際のアクセス制御処理時（ACL設定後の運用時）の処理として、実ユーザ名を確認するためにWWWサーバ13がディレクトリサーバ9のユーザ情報管理部25に問い合わせる方法を説明した。これに対して本実施形態では、確認すべきユーザの属性情報（ユーザ名やパスワードの情報など）およびユーザグループ情報（ユーザグループに所属するユーザのリスト）を、あらかじめWWWサーバ13に登録する方法について説明する。

【0102】図13は本発明の第5の実施の形態に係るアクセス制御設定システムの機能構成を示すブロック図であり、図2と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【0103】このアクセス制御設定システムは、設定管理サーバ8にユーザ情報送信部54、また各計算機12にユーザ情報設定部51が設けられるとともに、WWWサーバ13にユーザ情報データベース53が設けられる他、第1の実施形態と同様に構成されている。ここで、ユーザ情報データベース53は、一般的なWWWサーバが標準で持っている機構である。

【0104】ユーザ情報送信部54は、入力装置27から指定された部門に所属するユーザの属性情報とユーザグループ情報を、ユーザ情報管理部25から取得し、取得情報をネットワーク1を介してユーザ情報設定部51に送信する。ユーザ情報設定部51は、ユーザ情報送信部54から受け取った情報を、ユーザ情報データベース53に登録する。

【0105】次に、以上のように構成された本実施形態におけるアクセス制御設定システムの動作について説明する。まず、ACL設定処理については、第1の実施形態と同様であるのでその点は説明を省略する。

【0106】次に、アクセス権設定者は適宜のタイミング（例えばACL設定前の任意の時点やACL設定直後）で、入力装置27を介してユーザ情報送信部54に対象WWWサーバが必要とするユーザの属性情報とユーザグループ情報（例えば部門AのWWWサーバには、部門Aに属するユーザとユーザグループの情報を送信するなどの規則をあらかじめ定めておく。あるいはアクセス権設定者が指定する）を送信するよう指令する。

【0107】この指令を受けたユーザ情報送信部54により、ユーザ情報管理部25から必要なユーザの属性情報とユーザグループ情報が読み出され、対象部門のユーザ情報設定部51に送信される。ユーザ情報設定部51

は、受け取った情報を対象WWWサーバ13のユーザ情報データベース53に格納する。

【0108】次に、ACL設定されたコンテンツ28に対し、実際のシステム運用時にいかにしてアクセス制御するかを説明する。あるユーザがWWWサーバ13aのコンテンツ28aへアクセスしようすると、WWWサーバ13aがユーザに対してユーザ名とパスワードの入力を要求する。ユーザ名とパスワードをWWWサーバ13aが受け取ると、WWWサーバ13aは自己に設けられたユーザ情報データベース53に当該ユーザの属性情報を問い合わせ、ユーザ認証を行う。

【0109】このユーザ情報データベース53aから取得された実ユーザ名がACLと比較され、以下、第1の実施形態と同様にしてアクセス制御が行われることになる。上述した本発明の実施の形態に係るアクセス制御設定システムによれば、第1の実施形態と同様な効果が得られる他、第1～第4の実施形態とは異なる方式でアクセス制御を運用することができる。

【0110】なお、本実施形態は、第1の実施形態に対応させる場合を説明したが、本実施形態におけるユーザの属性情報を自己に設けられたユーザ情報データベース53から取得する方法は、他の第2、第3、第4実施形態に対しても適用することができる。これら各実施形態において、ユーザ情報送信部54、ユーザ情報設定部51及びユーザ情報データベース53を設けるようにすればよい。

(発明の第6の実施の形態) 上記各実施形態では、アクセス権設定パターン群24は予め設定されている物として説明したが、アクセス権設定パターンの生成・変更・削除を行うことも可能であり、本実施形態ではこの場合を説明する。

【0111】図14は本発明の第6の実施の形態に係るアクセス制御設定システムに適用されるアクセス権設定パターンの編集機能の構成を示すブロック図であり、図2～図13と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【0112】このアクセス制御設定システムは、第1～第5の何れかの実施形態に係るアクセス制御設定システムの設定管理サーバ8においてアクセス権設定パターン管理GUI61が設けられたものである。

【0113】この管理GUI61は、入力装置27から情報入力可能に構成され、同入力情報に基づくアクセス権設定パターンの生成・変更・削除をアクセス権設定パターン管理部23を介して行うようになっている。

【0114】このように構成された本実施形態のアクセス制御設定システムは、アクセス権設定パターンの生成・変更・削除の部分以外については第1～第5の実施形態と同様に動作する。管理GUI61の部分については以下のように動作する。

【0115】入力装置27から新しいアクセス権設定パ

ターンの情報(内容)が管理GUI61に入力されると、同GUI61によりアクセス権設定パターン群24に新たにパターンが追加される。

【0116】また、既存のアクセス権設定パターンの変更内容はアクセス権設定パターン管理部23及び管理GUI61を介して表示出力され、同表示を見ながら設定者62による変更入力となされる。この変更入力に基づき、管理GUI61によってアクセス権設定パターン群24の内容が変更される。

【0117】さらに、入力装置27から削除指令及び削除対象パターンの指定が入力されると、管理GUI61によって、アクセス権設定パターン群24から該当パターンが削除される。

【0118】上述した本発明の実施の形態に係るアクセス制御設定システムによれば、第1～第4の実施形態と同様な効果が得られる他、管理GUI61、入力装置27及びアクセス権設定パターン管理部23からなるアクセス権設定パターン管理機構を備えるようにしたので、アクセス権設定パターンの生成・修正・削除を容易に行うことができる。

【0119】また、アクセス権設定パターンの管理は、CUIベースでもGUIベースでも、両者を混合させた形でも行なうことができる。例えば管理GUI61及び入力装置27については、設定者62からのキーボード入力という形態であってもよく、また、表示面に対するマウスクリック及びキーボード入力という形態でもよく、種々の場合が考えられる。

(変形例) なお、本発明は、上記各実施の形態に限定されるものでなく、その要旨を逸脱しない範囲で種々に変形することが可能である。以下に変形の例を説明する。

【0120】【変形例1】実施形態では、ACL、ACLパターン、コンテンツ情報の送受信方法については特に記載していなかったが、これについては次のような形態が考えられる。必要な情報を正しく送受信できれば、何れの手法を用いてもよい。

【0121】・JavaRMI、あるいは、CORBA(Common Object Request Broker Architecture)に準拠したORB(Object Request Broker)技術などを利用した分散オブジェクト間のメッセージ通信を用いる。

【0122】・RPC(Remote Procedure Call)やSocketなどを用いたプロセス間通信を用いる。

・HTTP(Hyper Text Transfer Protocol)やCGI(Common Gateway Interface)など、一般的なWWWの機構を利用する。

【0123】・エージェントが必要な情報を保持し、配布して回る、等である。

【変形例2】実施形態では、アクセス権設定パターンにユーザ情報を適用することによりACLを生成しているが、すでに完成しているACLに相当するものをアクセス権設定パターンとして含めることもできる。この場合、ACL変換部22、22'では、選択されたアクセス権設定パターンをそのままACLとしてACL設定部15に送信することになる。

【0124】【変形例3】一つのアクセス権設定パターンの中に、抽象的なユーザ名と実ユーザ名（あるいはユーザグループ名）を混在させることもできる。この場合、抽象的なユーザ名のみがユーザ情報により変換され、はじめから実ユーザ名の部分はそのままの形のACLが生成される。

【0125】【変形例4】抽象的なユーザ名として、「部長」や「課長」など企業内の職制に関する例示を行ったが、抽象ユーザ名に特に制限はない。

【0126】【変形例5】実施形態では、アクセス権設定対象のリソースとして、WWWサーバ上のコンテンツについて記載したが、ファイルシステム上のファイルやデータベース上のデータ等、アクセス権の設定を行える計算機上のリソースであれば、対象となるリソースに関しての制限はない。

【0127】【変形例6】実施形態においては、アクセス権の設定・管理部門2を独立して設定したが、これがある部門、例えばA部門3が兼任するような形態にしてもよい。

【0128】【変形例7】図2～図11では、A部門3とB部門4の二つの部門が存在する形態で説明したが、図1に示すように部門数には特に制限はない。

【0129】【変形例8】第1の実施形態と、第2又は第3の実施形態を適宜組み合わせ、あるいは何れの実施形態を用いるかを適宜選択するようにすれば、アクセス権設定パターンからACLへの変換を設定・管理部門2で行なうか、設定対象の各部門3、4、...で行なうかを、システムの設計思想や負荷状況などによって選択することができる。

【0130】なお、本発明における記憶媒体としては、磁気ディスク、フロッピーディスク、ハードディスク、光ディスク（CD-ROM、CD-R、DVD等）、光磁気ディスク（MO等）、半導体メモリ等、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であってもよい。

【0131】また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているOS（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のMW（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行してもよい。

【0132】さらに、本発明における記憶媒体は、コン

ピュータと独立した媒体に限らず、LANやインターネット等により伝送されたプログラムをダウンロードして記憶又は一時記憶した記憶媒体も含まれる。

【0133】また、記憶媒体は1つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何らの構成であつてもよい。

【0134】なお、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであつて、パソコン等の1つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であつてもよい。

【0135】また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【0136】

【発明の効果】以上詳記したように本発明によれば、アクセス権設定パターンを予め設け、これを選択することでアクセスコントロールリストを生成するようにしたので、部門やサイトに依存せず効率的にリソースへのアクセス権を設定することを可能にし、ひいては設定の手間を軽減し設定ミスを防止できるアクセス制御設定システム及び記憶媒体を提供することができる。

【0137】また、アクセス権設定部に対する入力のみでアクセスコントロールリストを生成するとともに、生成したアクセスコントロールリストをリソースを管理する計算機側の設定手段でアクセス権設定できるようにしたので、設定対象の計算機にその都度ログインすることなしに当該設定を可能として、ひいては設定の手間を軽減し設定ミスを防止できるアクセス制御設定システム及び記憶媒体を提供することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態に係るアクセス制御設定システムを適用する計算機システムの構成例を示すブロック図。

【図2】同実施形態におけるアクセス制御設定システムの機能構成を示すブロック図。

【図3】アクセス権設定パターン群の一例を示す図。

【図4】ある部門（A部門）のユーザ情報の例を示す図。

【図5】他の部門（B部門）のユーザ情報の例を示す図。

【図6】ACL変換部により生成されるACLの例を示す図。

【図7】同実施形態のアクセス制御設定システムの動作を示す流れ図。

【図8】本発明の第2の実施の形態に係るアクセス制御設定システムの機能構成を示すブロック図。

【図9】同実施形態のアクセス制御設定システムの動作

を示す流れ図。

【図10】本発明の第3の実施の形態に係るアクセス制御設定システムの機能構成を示すブロック図。

【図11】本発明の第4の実施の形態に係るアクセス制御設定システムの機能構成を示すブロック図。

【図12】同実施形態のACL変換部により生成されるACLファイルの例を示す図。

【図13】本発明の第5の実施の形態に係るアクセス制御設定システムの機能構成を示すブロック図。

【図14】本発明の第6の実施の形態に係るアクセス制御設定システムに適用されるアクセス権設定パターンの編集機能の構成を示すブロック図。

【符号の説明】

- 1…ネットワーク
- 2…設定・管理部門
- 3…A部門
- 4…B部門
- 5…C部門
- 6…ルータ
- 7…データ伝送路
- 8…設定管理サーバ
- 9…ディレクトリサーバ
- 10…ルータ
- 11…データ伝送路
- 12…計算機
- 13, 13a, 13b…WWWサーバ
- 14…コンテンツ情報送信部
- 15…ACL設定部
- 21…アクセス権設定部
- 22, 22'…ACL変換部
- 23…アクセス権設定パターン管理部
- 24…アクセス権設定パターン群
- 25…ユーザ情報管理部
- 26…ユーザ情報
- 27…入力装置
- 28, 28a, 28b…WWWサーバ上のコンテンツ
- 29…生成されたACL
- 31…部門管理計算機
- 32…ACLパターン
- 51…ユーザ情報設定部
- 52…ユーザグループ名
- 53…ユーザ情報データベース
- 54…ユーザ情報送信部
- 61…管理GUI
- 62…設定者

11…データ伝送路

12…計算機

13, 13a, 13b…WWWサーバ

14…コンテンツ情報送信部

15…ACL設定部

21…アクセス権設定部

22, 22'…ACL変換部

23…アクセス権設定パターン管理部

24…アクセス権設定パターン群

25…ユーザ情報管理部

26…ユーザ情報

27…入力装置

28, 28a, 28b…WWWサーバ上のコンテンツ

29…生成されたACL

31…部門管理計算機

32…ACLパターン

51…ユーザ情報設定部

52…ユーザグループ名

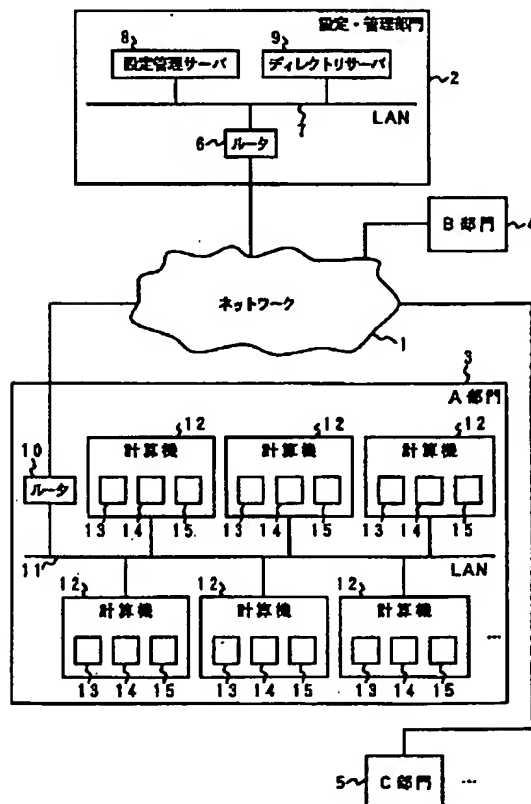
53…ユーザ情報データベース

54…ユーザ情報送信部

61…管理GUI

62…設定者

【図1】



【図3】

アクセス権	部長=読み出し権、課長=読み出し権
設定パターン#1:	システム管理者=読み出し権・実行権
アクセス権	部長=読み出し権・実行権、課長=読み出し権・実行権
設定パターン#2:	一般部員=読み出し権

【図4】

【図5】

部長	鈴木	部長	中村
課長	佐藤	課長	加藤
システム管理者	高橋、田中	システム管理者	斎藤
一般部員	渡辺、小林、伊藤	一般部員	佐々木、山本

【図12】

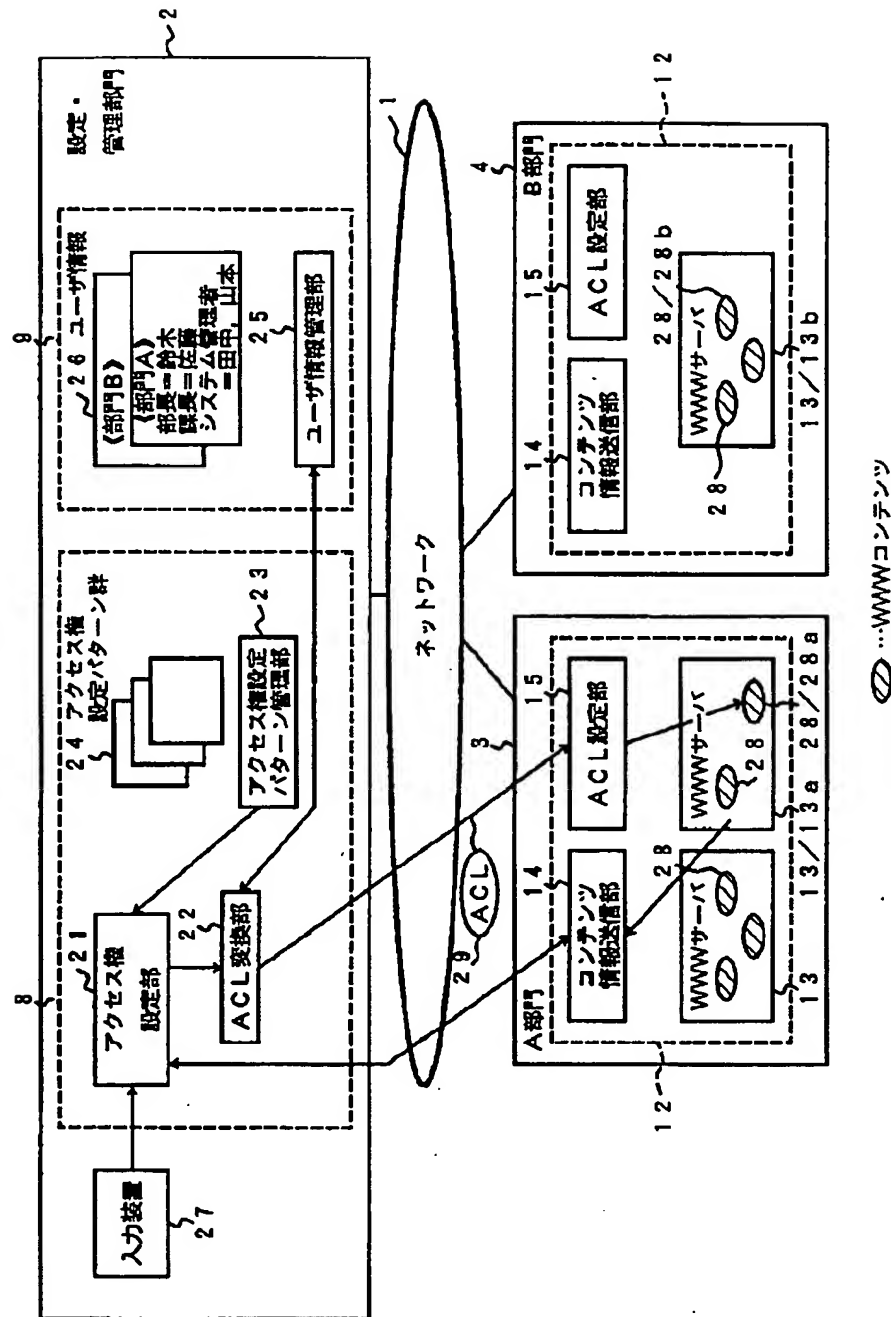
ACLファイルの例 (XXX.ac1)

```

path="/opt/www/docs/file1.html"
allow (read, write)
user="ユーザグループ名"
path="/opt/www/docs/file2.html"
allow ( ----- )
user( ----- )
:

```

【図2】



【図6】

(a) ACLファイルの例 (001.ac1)

```

path="/opt/www/docs/file1.html"
allow (read, write)
    user="yamada, tanaka"
path="/opt/www/docs/file2.html"
allow ( ..... )
    user=( ..... )
:

```

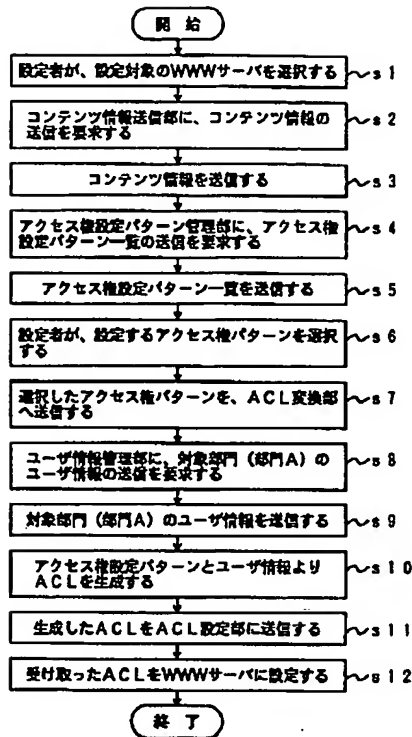
(b)

対象パス=0000
鈴木=読み出し権限
佐藤=読み出し権限
高橋=読み出し権限, 実行権限
田中=読み出し権限, 実行権限

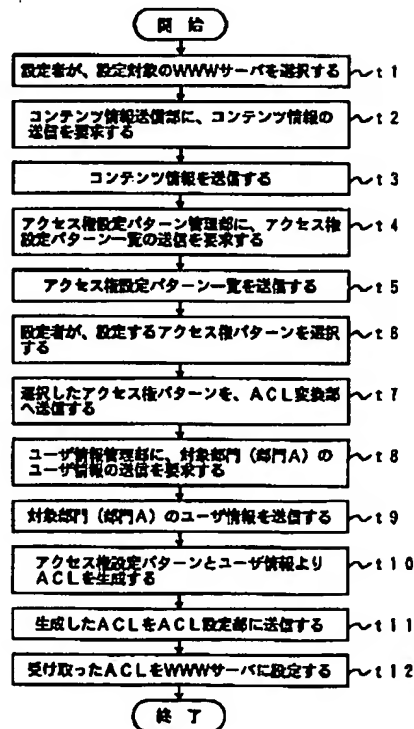
(c)

対象パス=xxxx
中村=読み出し権限
加藤=読み出し権限
斎藤=読み出し権限, 実行権限

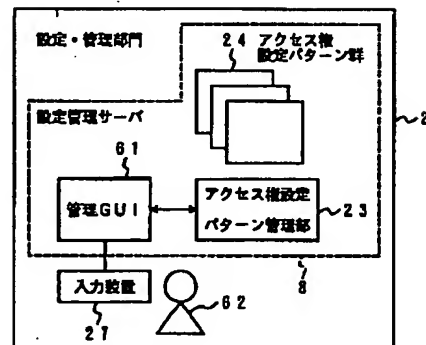
【図7】



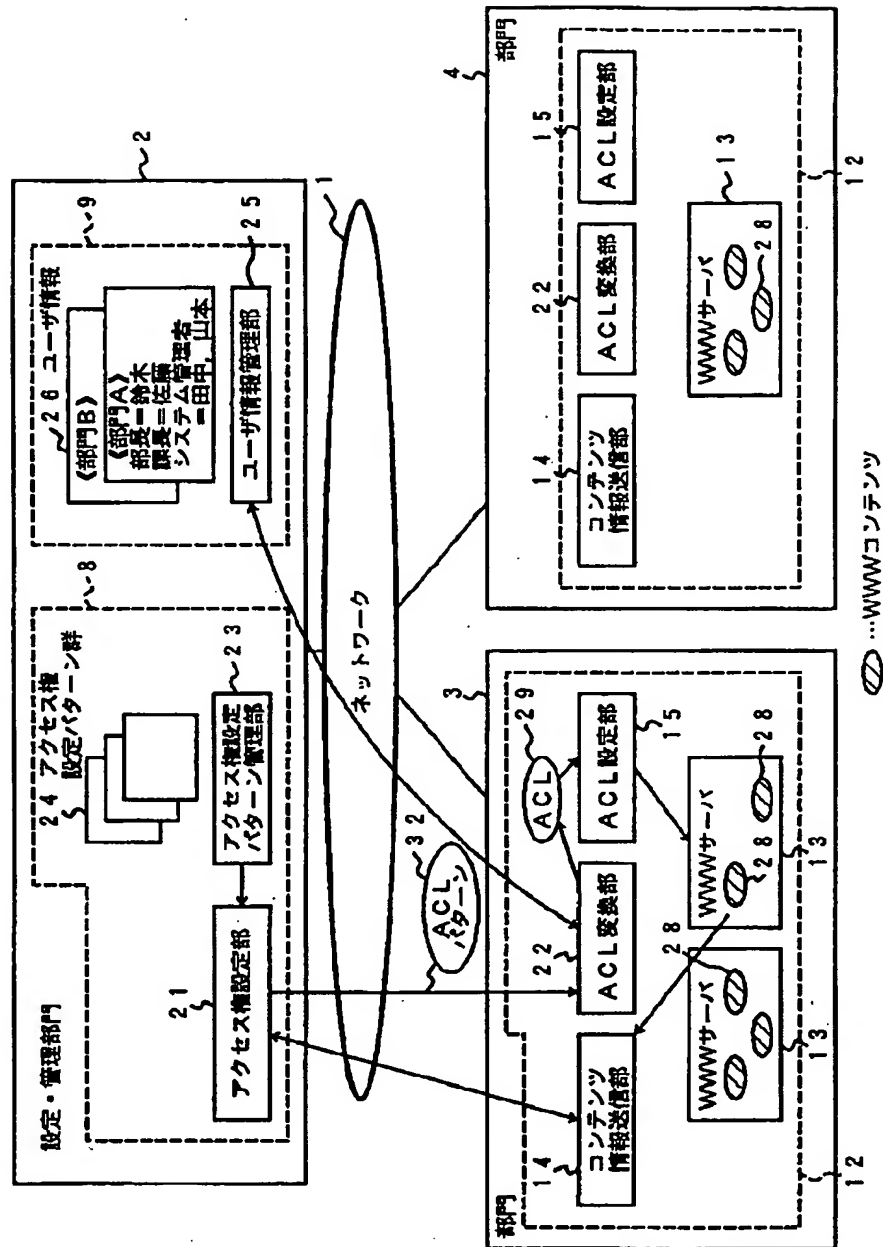
【図9】



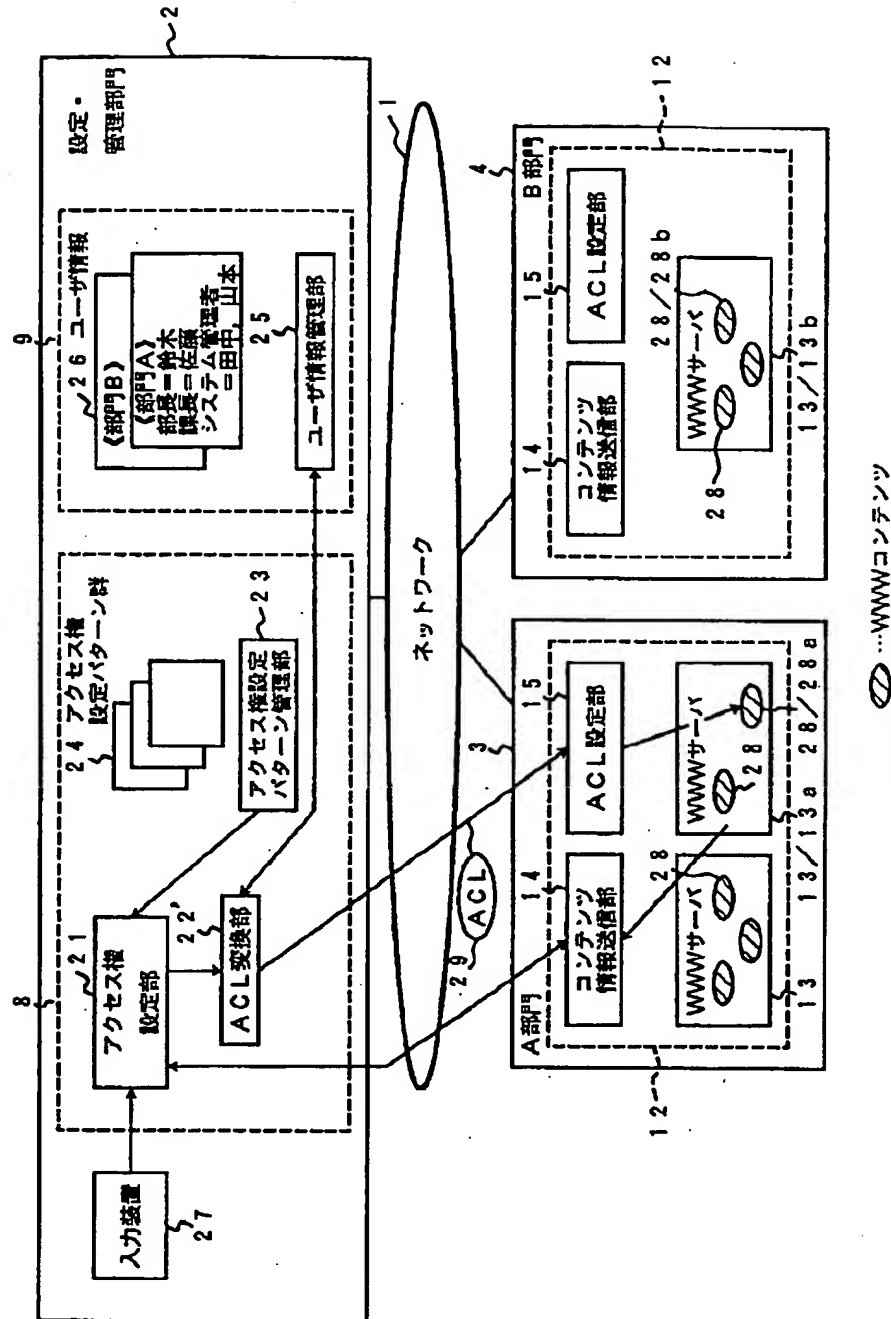
【図14】



【図10】



【図11】



【図13】

